DEFENDANT - SMF

EXHIBIT 2

Commonwealth of Pennsylvania
GOVERNOR'S OFFICE

EXECUTIVE ORDER

Subject:		Number:
Prohibition of Sexual Harassment in the Commonwealth		2002-4
Date: May 3, 2002	**Distribution:** B	**By Direction Of:** Mark S. Schweiker, Governor

WHEREAS, sexual harassment is a form of discrimination that undermines the integrity of the employment relationship and/or service delivery; and

WHEREAS, the Commonwealth of Pennsylvania, Pennsylvania's largest employer, has an obligation to assertively address sexual harassment issues in the workplace; and

WHEREAS, sexual harassment shall not be tolerated in Commonwealth workplaces under any circumstances; and

WHEREAS, this Administration is committed to providing a work environment where employees, applicants for employment, or individuals receiving services from the Commonwealth shall not be subjected to sexual harassment; and

WHEREAS, to prevent sexual harassment in the workplace, all managers, supervisors, and employees must be made aware of the Commonwealth's sexual harassment policy, the steps to take when concerns arise, and our commitment to address instances of sexual harassment aggressively and equitably.

NOW, THEREFORE, I, Mark S. Schweiker, Governor of the Commonwealth of Pennsylvania, by virtue of the authority vested in me by the Constitution of the Commonwealth of Pennsylvania and other laws, do hereby adopt and reaffirm the Commonwealth's sexual harassment policy as follows:

1. No department, board, commission, or other agency under my jurisdiction shall tolerate sexual harassment by any Commonwealth employee against any other employee, applicant for employment, or client or other person receiving services from or conducting business with the Commonwealth. Sexual harassment in Commonwealth work settings is strictly forbidden. Further, no department, board, commission, or other agency under my jurisdiction shall tolerate acts of sexual harassment by persons not employed by the Commonwealth within Commonwealth offices or upon employees of the Commonwealth in the performance of their duties. Sexual harassment is a violation of federal and state law. Therefore, all federal and state laws relating to sexual harassment and/or sex discrimination will be enforced.

2. Sexual harassment includes unwelcome sexual advances, requests for sexual favors, and/or other verbal, visual, or physical conduct of a sexual nature where:

a. submission to or rejection of such conduct is made either explicitly or implicitly a term or condition of an individual's employment; or

EXHIBIT 1

b. submission to or rejection of such conduct by an individual is used as a basis for employment decisions affecting such individuals; or

c. such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

Prohibited sexual harassment may include actions by members of the opposite sex of an employee as well as members of an employee's own sex. Prohibited sexual harassment may include actions which are overtly sexual or facially neutral if such actions constitute gender-based discrimination.

3. Any Commonwealth employee who engages in or knowingly condones sexual harassment related to Commonwealth employment shall be subject to disciplinary action, up to and including dismissal.

4. Retaliation in any form against an employee, applicant for employment, client, or person conducting business with or receiving services from the Commonwealth who exercises his or her right to make a good faith complaint under this policy or who cooperates in an investigation of any complaint is strictly prohibited, and will itself be cause for appropriate disciplinary action.

5. All Commonwealth employees will be educated in sexual harassment issues. Education may consist of written materials, formal training, educational videos, orientation sessions, workplace discussions, and/or individual counseling. All Commonwealth employees will be provided with a copy of this policy and must sign an acknowledgement that they have received and reviewed the policy.

6. Agency heads shall create a workplace environment which encourages discussion of sexual harassment issues, where employees are educated and sensitized to sexual harassment, and where individuals with sexual harassment questions or complaints are provided with a response which is clear, impartial, and timely.

7. The Secretary of Administration shall require each agency to have an effective complaint mechanism which ensures that an employee does not have to complain to the alleged harasser and which provides for prompt and effective investigation of complaints. The Secretary of Administration shall also have the authority to issue Management Directives and establish rules necessary to carry out the mandates of this Executive Order.

8. The Office of Administration, Bureau of Equal Employment Opportunity, shall provide appropriate oversight and resolution of such complaints.

9. This *Executive Order* and *Management Directive 505.30, Prohibition of Sexual Harassment in Commonwealth Work Settings,* constitute the Commonwealth's sexual harassment policy.

10. **Cooperation by State Agencies.** All Commonwealth departments, boards, commissions, and other agencies under my jurisdiction shall cooperate fully with the Secretary of Administration and provide such assistance and information, as needed, in the implementation of this order.

11. **Effective Date.** This order shall take effect immediately.

12. **Rescission.** *Executive Order 1999-3, Prohibition of Sexual Harassment in the Commonwealth.*

MANAGEMENT DIRECTIVE

505.30
Amended
Number

COMMONWEALTH OF PENNSYLVANIA
GOVERNOR'S OFFICE

Subject:

Prohibition of Sexual Harassment in Commonwealth Work Settings

By Direction Of: Fritz Bittenbender, Secretary of Administration

Date: June 19, 2002

This directive provides detailed policy and procedures to fulfill the mandate expressed in *Executive Order 2002-4, Prohibition of Sexual Harassment in the Commonwealth.* This directive requires all employees under the jurisdiction of the Governor to read and sign a copy of Enclosure 1. The signed copy should be given to the employee's supervisor and is to be maintained in the employee's Official Personnel Folder. This amendment contains minor changes.

1. PURPOSE. To announce the Commonwealth's policy on sexual harassment, define sexual harassment, and identify steps which agencies should take to reduce the chances of sexual harassment occurring.

2. SCOPE. This directive applies to all departments, boards, commissions, and other agencies under the Governor's jurisdiction and to all employees of those agencies.

3. OBJECTIVES.

a. Define the Commonwealth's policy on sexual harassment.

b. Outline reporting procedures for violations of policy on sexual harassment.

c. Define the Commonwealth's policy on retaliation regarding sexual harassment.

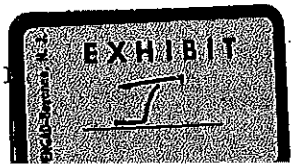
d. Provide an acknowledgment procedure to ensure that employees are aware of the policy on sexual harassment.

4. POLICY.

a. *Executive Order 2002-4* and this directive constitute the Commonwealth's sexual harassment policy. The policy is based on federal and state law, court decisions, and a commitment that sexual harassment will not be tolerated in Commonwealth workplaces and work settings. Sexual harassment in the workplace is a form of employment discrimination.

b. It is the policy of the Commonwealth of Pennsylvania that sexual harassment of employees, applicants for employment, or clients of or individuals conducting business with or receiving services from the Commonwealth is strictly prohibited and will not be tolerated.

c. Sexual harassment is a violation of state and federal law. Therefore, all federal and state laws relating to sexual harassment or sex discrimination, or both, will be enforced. Under this policy, all employees share responsibility for ensuring that the workplace is free from all forms of sexual harassment.



d. The Commonwealth will not tolerate sexual harassment by any employee against another employee, applicant for employment, client of or any person conducting business with or receiving services from the Commonwealth or any representative thereof.

e. Individuals not employed by the Commonwealth will be held responsible for any acts of sexual harassment they may commit within the Commonwealth work settings or upon employees of the Commonwealth while in the performance of their duties.

f. Any employee who engages in or knowingly condones sexual harassment shall be subject to disciplinary action, up to and including dismissal.

g. Retaliation in any form against an employee or applicant, or against any client or other person receiving services or conducting business with the Commonwealth, who exercises his or her right to make a complaint under this policy or who cooperates in the investigation of any such complaint is strictly prohibited, and will itself be cause for appropriate disciplinary action. Any employee who believes that he or she has been the victim of retaliation should report his or her concerns as stated in Section 7.a.

5. DEFINITION. Sexual harassment includes unwelcome sexual advances, requests for sexual favors, and/or other verbal, visual, or physical conduct of a sexual nature where:

a. submission to or rejection of such conduct is made either explicitly or implicitly a term or condition of an individual's employment; or

b. submission to or rejection of such conduct by an individual is used as a basis for employment decisions affecting such individuals; or

c. such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive work environment.

EXAMPLES

Examples of acts of sexual harassment which shall not be tolerated include, but are not limited to the following, particularly when they are repeated or part of a general pattern of behavior:

Written: Unwelcome suggestive, sexually explicit, or obscene letters, poems, notes, or invitations.

Verbal: Derogatory, sexually explicit, or offensive comments, epithets, slurs or jokes; inappropriate comments about an individual's body or sexual activities; repeated unwelcome propositions or repeated sexual flirtations; direct or subtle pressures or repeated unwelcome requests for dates or sexual activities.

Physical: Impeding or blocking movements, touching, patting, pinching, or any other unnecessary or unwanted physical contact.

Visual: Sexually oriented gestures, display of sexually suggestive or derogatory objects, pictures, cartoons, posters, or drawings.

Prohibited sexual harassment may include actions by members of the opposite sex of an employee as well as members of an employee's own sex. Managers and supervisors are responsible for inspecting their respective work areas for materials which might be offensive to others and for removing all such materials. Prohibited sexual harassment may include actions which are overtly sexual or facially neutral if such conduct constitutes gender-based discrimination.

No manager, supervisor, or other employee shall threaten or suggest, either explicitly or implicitly, that the refusal by another employee or applicant for employment to submit to sexual advances in any form will adversely affect that person's employment, performance evaluation ratings, wages, compensation, advancement, assigned duties, work assignments, work schedules, training, or any other term or condition of employment or career development. In addition, offering, promising, or granting favored treatment

to any employee or applicant for employment as a result of that person's engaging in or agreeing to engage in sexual conduct, as well as seeking in any way to make the performance of a person's job more difficult because of that person's refusal to submit to sexual advances are strictly prohibited.

6. RESPONSIBILITIES.

a. **The Secretary of Administration** shall require each agency to have an effective complaint mechanism which ensures that an employee does not have to complain to the alleged harasser and which provides for prompt and effective investigation of complaints.

b. **Agency heads** shall:

(1) Support the Commonwealth's sexual harassment policy and reinforce that support, in writing, to their employees. However, agency heads should not restate the policy in different words in written transmittals. It is important that the wording used in this directive and *Executive Order 2002-4* be consistently used and applied among all agencies under the Governor's jurisdiction.

(2) Ensure that all employees under their jurisdiction are educated in the Commonwealth's sexual harassment policy and in sexual harassment issues in general. Education may consist of written materials, formal training, educational videos, orientation sessions, workplace discussions, and/or individual counseling. Education in sexual harassment issues should be considered an ongoing effort, with additional approaches used periodically to reinforce earlier education.

(3) Disseminate names and phone numbers for the agency's Equal Opportunity Manager/Specialist or Human Resource Director or any other individual to whom an employee may report allegations of sexual harassment.

c. **The Office of Administration, Bureau of Equal Employment Opportunity,** shall make available resources to supplement agency educational efforts.

7. PROCEDURES.

a. **Reporting Violations of Policy on Sexual Harassment.** Any employee who believes that he or she has been the victim of sexual harassment in any form, by any manager, supervisor, coworker, customer, client, or any other person in connection with his or her employment should bring the problem immediately to the attention of his or her supervisor or someone in the employee's direct line of supervision. If the concern involves the employee's direct supervisor or someone in the employee's direct line of supervision, or if the employee is uncomfortable for any reason with discussing such matters with the supervisor and/or others in the direct line of supervision, or is not satisfied after bringing the matter to such individuals, the employee may take his or her concerns to the agency Equal Opportunity Manager/Specialist or Human Resource Director or other individual designated by the agency head under Section 6.b.(3).

All allegations of sexual harassment will be investigated in a confidential manner. Sexual harassment complaints do not have to be in writing before an investigation is initiated. When warranted, all appropriate corrective action will be taken. Any employee who is found, as a result of such investigation, to have engaged in sexual harassment in violation of this policy is subject to appropriate disciplinary action, up to and including termination of employment. A manager or supervisor will be subject to appropriate disciplinary action, up to and including termination of employment, if he or she fails to take corrective action when it is known, or reasonably should have been known, that an individual in the line of supervision of the manager or supervisor is or was being sexually harassed.

b. **Acknowledgment of Receipt of Enclosure 1.** Every Commonwealth employee is to be provided with a copy of *Executive Order 2002-4* and this directive. Each employee is asked to read the documents and sign a copy of Enclosure 1, Acknowledgment of Receipt of the Commonwealth of Pennsylvania's Sexual Harassment Policy. Signed copies of the form contained in Enclosure 1 are to be maintained in the employee's Official Personnel Folder. (STD-301) by the agency human resource office. The form may be photocopied and provided to the employee for signature.

c. **Dissemination.** In addition to the dissemination of Enclosure 1, the sexual harassment policy contained in *Executive Order 2002-4* and this directive should be disseminated to all employees by:

(1) Posting the policy in conspicuous places throughout the workplace.

(2) Placing the policy in all employee handbooks and/or policy manuals.

(3) Distributing the policy during new employee orientation programs.

(4) Redistributing the policy each year.

(5) *Executive Order 2002-4* and this directive can be accessed on the State's Home Page, **www.state.pa.us.** At the top of the screen, go to the block "PA Keyword." Type in Executive Orders or Management Directives (whichever applies). Then, scroll down to the document by the number of the document.

d. Any Commonwealth employee who engages in or knowingly condones sexual harassment related to Commonwealth employment shall be subject to disciplinary action, up to and including dismissal.

Enclosure:

1 – Acknowledgment of Receipt of the Commonwealth of Pennsylvania's Sexual Harassment Policy

This directive supersedes Management Directive 505.30 dated May 13, 1999. Please recycle the previous version.

DEFENDANT - SMF

EXHIBIT 3

DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
OFFICE OF THE ADJUTANT GENERAL
COMMONWEALTH OF PENNSYLVANIA
FORT INDIANTOWN GAP
ANNVILLE, PENNSYLVANIA 17003-5002
www.dmva.state.pa.us

12 February 2014

PROHIBITION OF SEXUAL HARASSMENT

Sexual harassment is a form of unlawful discrimination that undermines the integrity of the employment relationship. Sexual harassment will not be tolerated in any Department of Military and Veterans Affairs (DMVA) or Pennsylvania National Guard workplace under any circumstances.

Sexual harassment is a violation of federal and state law and Commonwealth policy. Sexual harassment includes unwelcome sexual advances, requests for sexual favors, and/or other verbal, visual, or physical conduct of a sexual nature where:

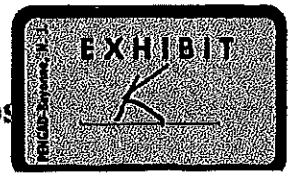
- Submission to or rejection of such conduct is made either explicitly or implicitly a term or condition of an individual's employment; or
- Submission to or rejection of such conduct by an individual is used as a basis for employment decisions affecting such individuals; or
- Such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

All allegations of sexual harassment will be investigated promptly. Investigations will be conducted in as confidential a manner as possible under applicable laws and regulations. Sexual harassment complaints do not have to be in writing before an investigation is initiated. When warranted by the facts and circumstances, all appropriate corrective action will be taken. Any employee who engages in or knowingly condones sexual harassment related to Commonwealth employment will be subject to disciplinary action, up to and including termination of employment.

DMVA employees should report any instances of sexual harassment. Any employee who believes that he or she has been the victim of sexual harassment in any form, by any manager, supervisor, co-worker, customer, client or any other person in connection with his or her employment should bring the problem immediately to the attention of his or her supervisor or someone in the employee's direct line of supervision. If the concern involves the employee's direct supervisor or someone in the employee's direct line of supervision, or if the employee is uncomfortable for any reason with discussing such matters with the supervisor and/or others in the direct line of supervision, or is not satisfied after bringing the matter to such individuals, the employee may take his or her concerns to the agency Equal Opportunity Officer.

Lori S. Millar is designated as the DMVA Equal Opportunity Officer to whom employees may report any instances of sexual harassment. *Ms. Millar can be reached at 717-861-8796 or at lmillar@pa.gov*

TO BE PERMANENTLY POSTED ON ALL DMVA BULLETIN BOARDS



In addition, complaints may be filed with the following agencies:

Within 90 days of Incident:
Department of Military and Veterans Affairs
Office of Administration - HR
Div. of Training & Equal Emp. Opportunity
Bldg 0-47 Fort Indiantown Gap
Annville, PA 17003-5002
(717) 861-8796
(717) 861-6200 Fax

Within 20 days of incident if employee is designated as Civil Service:
State Civil Service Commission
Strawberry Square, 4th Floor
320 Market Street, Appeals Office
Harrisburg, PA 17108-0569
(717) 783-1444
(717) 787-8650 Fax
(717) 772-2685 TTD

Within 180 days of incident:
PA Human Relations Commission
Executive Offices
333 Market St., 8th Floor
Harrisburg, PA 17126-0333
(717) 787-4410
(717) 787-7279 TTY users only
(717) 772-4340 Fax

Within 300 days of incident:
Equal Employment Opportunity Commission
Philadelphia District Office of Administration
801 Market Street, Suite 1300
Philadelphia, PA 19107-3127
(800) 669-4000
(800) 669-6820 TTY
(215) 440-2606 FAX

Important Commonwealth policies and procedures on prohibiting sexual harassment are contained in Executive Order 2002-4 (Prohibition of Sexual Harassment in the Commonwealth) and Management Directives 505.30 and 505.30 Rev. No. 1 (Prohibition of Sexual Harassment in Commonwealth Work Settings). DMVA employees should review these documents and be familiar with how to deal with sexual harassment in work settings. Acknowledgement of Receipt of the Commonwealth of Pennsylvania's Sexual Harassment Policy will be administered electronically and/or manually.

Any DMVA employee who witnesses sexual harassment should immediately contact his or her supervisor or someone in the employee's direct line of supervision or the appropriate designated agency Equal Opportunity Officer. Any manager or supervisor who becomes aware of possible workplace sexual harassment must take immediate action and report it to the Equal Opportunity Officer.

Retaliation in any form against anyone who exercises his or her right to make a good faith complaint or who cooperates in an investigation is strictly prohibited and is subject to disciplinary action.

Remember: Sexual harassment is illegal, and it is wrong. It disrupts the workplace and interferes with our jobs to serve Pennsylvania Veterans and our Soldiers and Airmen. DMVA will not tolerate sexual harassment in any form. If you are a victim of sexual harassment or a witness to sexual harassment in the workplace, report it immediately. Working together, we can and will maintain a workplace free of sexual harassment and all forms of unlawful discrimination.

Wesley E. Craig
Major General, PA Army National Guard
The Adjutant General

TO BE PERMANENTLY POSTED ON ALL DMVA BULLETIN BOARDS

DEFENDANT - SMF

EXHIBIT 4

pennsylvania
DEPARTMENT OF MILITARY
AND VETERANS AFFAIRS

Policy
Information
Memorandum

Number: 09-008	Last Issue Date: **August 12, 2011** **Revised: January 28, 2014**	Effective Date: **January 28, 2014**

Subject:	Distribution:
Workplace Violence and Workplace Bullying Prevention Policy	All DMVA Commonwealth Employees
References: • TAG Workplace Violence Policy • Management Directive 205.33, *Workplace Violence*	By Direction of: Dee McPherson Deputy for Administration

PURPOSE

The Department of Military and Veterans Affairs (DMVA) strives to ensure a safe work environment for all employees. A workplace violence prevention program has been developed to address guidelines to prevent incidents of violence in the workplace and to establish procedures for incident response and reporting. This program includes major elements such as definitions of workplace violence, program requirements and roles and responsibilities; as well as employee training and annual program evaluation.

OBJECTIVE

The goal is to prevent workplace violence and to provide a safe work environment for our employees, visitors, residents and their families. The purpose of this policy is to establish the methods used for developing, communicating, and evaluating the agency's workplace violence prevention program goals and objectives. At a minimum, the workplace violence program must include:

1. Workplace violence policy
2. Security policy and plan for workplace violence threats and incidents
3. Work environment that emphasizes health and safety
4. Employee training

Employees have a responsibility to treat each other, their supervisors, residents and the public with respect and courtesy. The Department of Military and Veterans Affairs (DMVA) affirms that all employees at all levels of the Department must avoid intimidating, hostile, and/or inappropriate behaviors while on duty, as a result of performing their duty or in a Commonwealth workplace. Such behavior can include but is not limited to threats in person, by letter or note, telephone, fax or electronic mail, threatening gestures or expressions that communicate a direct or indirect threat of physical harm; abusive language, poor on-the-job relationships; fighting, bullying, theft or destruction of Commonwealth property.

EXHIBIT 2

DEFINITIONS

Workplace
A workplace is any Commonwealth owned or leased property, location where Commonwealth business is conducted, or site where an employee is considered "on duty". Commonwealth vehicles or private vehicles being utilized for Commonwealth business are included in this definition. Additionally, workplace violence can occur at any location if the violence has resulted from an act or decision made during the course of conducting Commonwealth business.

Inappropriate Workplace Behavior
Inappropriate behavior includes actions unacceptable for the workplace. Inappropriate workplace behavior may include attendance problems, decreased productivity, inconsistent work patterns, poor on-the-job relationships, unusual/changed behavior, personal conflicts, disruptive behavior and fighting.

Violence
Violence connected to the workplace takes many forms. Incidents of workplace violence include but are not limited to, threats in person, by letter or note, telephone, fax or electronic mail, intimidation, harassment (to include sexual harassment), mugging, robbery and attempted robbery and destruction of Commonwealth property. Cases that are considered extremely serious include, but are not limited to, physical assault, rape, murder or bomb threats. Incidents may take place between employees, employees and clients, employees and acquaintances/partners and employees and strangers. Incidents of workplace violence may occur at or away from the workplace. The determining factors in assessing whether an incident constitutes workplace violence are the individuals involved and the relationship of the action to the workplace, the location of the incident and/or if the violence is a result of Commonwealth business.

Bullying
Workplace bullying is repeated, health-harming mistreatment, verbal abuse or conduct which is threatening, humiliating and or intimidating. Bullying also includes sabotage that interferes with work or exploitation of a known psychological or physical vulnerability. Workplace bullying can lead to instances of workplace violence.

State Employee Assistance Program (SEAP)
A program for state employees designed to assist them and their families with substance abuse, emotional, family, financial, marital and/or personal problems. All employees, supervisors, managers and union stewards are encouraged to utilize the services of SEAP when personal problems first develop; regardless of any job performance concerns.

Protection From Abuse Orders (PFA)
In order to protect employees at the workplace, employees who have PFA orders from other individuals are encouraged to notify their supervisors or managers. Due to the confidentiality and sensitivity of domestic violence, managers and supervisors shall remain flexible to assist an employee who self-discloses domestic violence, take appropriate steps to minimize the opportunity for the legally identified perpetrator to contact or visit the employee and encourage the employee to seek assistance through the State Employee Assistance Program (SEAP) at 1-800-692-7459.

POLICY

There are five (5) essential components of a comprehensive workplace violence prevention program:

1. **Management Commitment and Employee Involvement**

   Management commitment and employee involvement are complementary and essential to a successful workplace violence prevention program. Management commitment provides the motivating force for dealing effectively with workplace violence and workplace bullying. Employee involvement enables workers to develop and express their commitment to safety and health.

   a. Management commitment must be evident in the form of high-level management involvement and support for a written workplace violence prevention policy and its implementation, joint management-worker violence prevention committees, post-assault counseling, debriefing and follow-up.
   b. Employees must participate in hazard assessment and problem solving activities.
   c. Report all incidences of Workplace Violence or Workplace Bullying.

2. **Worksite Analysis**

   a. Conduct regular walk-through surveys of the workplace.
   b. Collection and review of all reports of worker assault.
   c. A successful job hazard analysis must include strategies and policies for encouraging the reporting of all incidents of workplace violence; including verbal threats that do not result in physical injury.

3. **Hazard Prevention and Control**

   a. Establishment for responding to acts of violence.
   b. Hazard prevention and control includes the installation of equipment, such as alarm systems in high-risk areas.
   c. Security policy and plan for workplace violence threats and incidents.

4. **Safety and Health Training**

   Training and education must include pre-placement and periodic, educationally-appropriate training regarding the risk factors for violence in the health care environment and control measures available to prevent violent incidents. Training should include skills in aggressive behavior identification and management.

5. **Recordkeeping and Program Evaluation**

   a. Perform an annual self-assessment of the workplace violence prevention program to evaluate effectiveness. Evaluation will include a full review of the prior year's statistics.

b. Determine if the original solutions have been successful in reducing the frequency and severity of injuries in the workplace, identify any unforeseen problems and explore areas for further improvement.
c. Discuss and implement changes, where necessary, in order to reduce potential for these incidents. Revise the action plan to reflect ongoing changes and updates.

RESPONSIBILITIES

Agency Workplace Violence Coordinator

- Implement the provisions of the management directive, workplace violence prevention initiatives and training agency-wide; provide information and assistance on workplace violence issues and questions to all managers, supervisors and employees; and report incidents of workplace violence to the Governor's Office of Administration.

Safety Committee Members

- A key element of the workplace violence prevention program is the health and safety committee. The primary function of the committee is to provide a thorough workplace security/hazard analysis and establish prevention strategies. An effective committee will assess the organization's vulnerability to workplace violence, make recommendations for preventive actions and employee training programs in violence prevention and evaluate the overall workplace violence prevention program on a monthly basis; in conjunction with the safety committee meetings held in each facility.
- Review on a monthly basis all Workplace Violence incidents.

Managers/Supervisors

- Support the implementation of the Workplace Violence and Workplace Bullying Prevention Policy.
- Participate in hazard assessment and problem solving activities of the Workplace Violence Prevention Program.
- Ensure that staff attends and participates in workplace violence/bullying prevention.
- Immediately report all Workplace Violence and Workplace Bullying incidents to their Human Resources Office.

Employees

- Understand and comply with the Workplace Violence Prevention Program and other safety and security measures.
- Participate in employee complaint or suggestion procedures covering safety and security concerns.
- Reporting violent incidents or incidents of bullying promptly and accurately.
- Participate in safety and health committees or teams that receive reports of violent incidents or security problems and respond with recommendations for corrective strategies.

- Employees who have PFA orders from other individuals should notify management immediately. Employees should work with their managers and supervisors to take appropriate steps to minimize the opportunity for the legally identified perpetrator to contact or visit the employee.
- Take part in available training courses that covers techniques to recognize escalating agitation, high risk behavior or criminal intent and discusses appropriate responses.

Agency SEAP Coordinator

- Notify HR-Agency SEAP designee when warning signs and inappropriate behavior first develop as an attempt at early intervention.
- Notify HR-Agency SEAP designee following a serious incident of workplace violence and coordinate a debriefing where warranted.
- Notify agency workplace violence coordinator; maintaining the confidentiality of the incident.
- Inform managers and supervisors of the resources provided by SEAP, should an incident of workplace violence occur.

PROCEDURES

- Employees exhibiting early warning signs of potential violence, such as personal conflict or disruptive behavior, should be counseled and confidentially informed of services provided by SEAP. The supervisor should take appropriate administrative and disciplinary action consistent with the seriousness of the behavior.
- When employees exhibit signs of inappropriate workplace behavior which create a clear and present danger, give rise to the concerns of imminent danger, to self or others, such as threats, physical confrontation, assault or other violent actions, an immediate response is required by the supervisor
- Training classes and/or workshops on workplace violence are to be made available, as appropriate, through the agency's workplace violence coordinator. All managers, supervisors, union stewards, Health and Safety Committee members and employees with high levels of interaction with the public should attend training. Information on workplace violence should be made available to all employees, including the distribution of reading materials and appropriate workplace discussions.
- Employees, supervisors and managers who witness or experience any workplace violence situation, including threats of violence, must report the incident to their Human Resource Office. All incidents and suspected incidents of workplace violence, as defined in this policy, must be reported.

AWARENESS, EDUCATION AND TRAINING

All current and new employees are to receive workplace violence information to review and to utilize in case of a workplace violence incident. Training for *new* employees should occur during the orientation process. Training for *current* employees should be made available on an annual basis. This training should include bomb threats, workplace violence prevention and reporting workplace violence.

DEFENDANT - SMF

EXHIBIT 5

MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania
Governor's Office

Subject: Workplace Violence	***Number:*** 205.33 Amended
Date: June 16, 2014	***By Direction of:*** Kelly Powell Logan, Secretary of Administration

Contact Agency:
Office of Administration, Office for Human Resources Management, Bureau of Employee Benefits and Services, Telephone 717 787 8575

This directive establishes policy, responsibilities, and procedures on preventative measures and responses to violence in the workplace. Marginal dots are excluded due to major changes.

1. **PURPOSE.** To establish policy, responsibilities, and procedures to prevent incidents of violence in the workplace and for incident response and reporting.

2. **SCOPE.** This directive applies to all departments, boards, commissions, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction. Independent agencies are encouraged to comply with this directive.

3. **OBJECTIVE.** To provide policy and procedures for commonwealth agencies and employees to promote a workplace which is free of violence.

4. **DEFINITIONS.**

   a. **Domestic Violence.** Violence that occurs between individuals who have or had a significant personal relationship.

   b. **Employee.** A person who has been hired by an agency subject to *"The Administrative Code of 1929," Act 175 of 1929, P.L. 177; 71 P.S. § 51,* and whose employment has not yet been terminated.

EXHIBIT M

c. **Inappropriate Workplace Behavior.** Employee actions which are inappropriate or unacceptable for the workplace but which do not rise to the level of workplace violence. Examples include, but are not limited to, time and attendance problems, decreased productivity, inconsistent work patterns, poor on-the-job relationships, unusual/changed behavior, personal conflicts, and disruptive behavior.

d. **Protection From Abuse Order (PFA).** A legal document that prevents one individual from having contact with or being within a specified distance of another individual.

e. **State Employee Assistance Program (SEAP).** A program designed to assist state employees and their families with alcohol, drug, emotional, family, financial, marital, or personal problems. Policy and procedures are contained in *Executive Order 1996-10*, *Management Directive 505.22*, and *Manual 505.3*, all titled *State Employee Assistance Program.*

f. **Violence.** Behavior that results in physical harm to an individual or property, emotional harm to an individual, or the threat of such harm to an individual or property.

g. **Warning Signs.** An observable behavior which may indicate that an individual may be a higher risk for committing an act of workplace violence. Warning signs may include; but are not limited to, overreacting, offensive or profane language, rapid speech, continual blame or excuses, being overly defensive when criticized, or repeated unusual movements such as pounding, banging, or slamming.

h. **Workplace.** A location where employees perform job duties. The location need not be a permanent location, physical building, or commonwealth-owned property.

i. **Workplace Violence.** Violence that occurs at or is connected to the workplace, including any location if the violence has resulted from an act or a decision made during the course of conducting commonwealth business. Examples of workplace violence include but are not limited to: verbal and written threats, intimidation, stalking, harassment, domestic violence, robbery and attempted robbery, destruction of commonwealth property, physical assault, bomb threats, rape and murder. Perpetrators of workplace violence can include employees, clients/customers, personal acquaintances/partners and strangers.

j. **Zero Tolerance.** All reported incidents of workplace violence will be investigated. Appropriate action(s), up to and including termination of employment, and potential legal action, will be taken for all incidents where an investigation has determined that workplace violence has occurred.

5. **POLICY.**

a. Workplace violence by or against commonwealth employees is prohibited. The commonwealth has a "zero tolerance" policy for incidents of workplace violence.

b. Violations of this policy by a commonwealth employee may lead to disciplinary action, up to and including termination from employment. The employee may also be subject to criminal prosecution.

c. Law enforcement employees who use force within their line of work are not in violation of this directive, so long as their actions are in compliance with applicable statutes and agency policies.

d. All managers, supervisors, and employees are to be made aware of the commonwealth and agency policies on workplace violence and are required to receive training on workplace violence prevention and response.

e. The commonwealth recognizes the sensitivity of domestic violence, the challenges in ending such violence, and the need for a coordinated effort of support and resources. As such, no commonwealth employee shall be required to disclose that he or she is a victim of domestic violence or has filed a PFA. Employees who make such a self-disclosure shall be referred to SEAP, shall not be discriminated against for such self-disclosure, and shall be afforded the same level of confidentiality as any other individual seeking assistance for a personal issue.

f. Agencies are to remain flexible in order to assist employees who self-disclose that they are victims of domestic violence, subject to operational efficiency and existing collective bargaining agreements, including:

(1) Approval of paid and unpaid leave.

(2) Relocation of current work space within the existing office building, or temporary or permanent transfer to an alternate work location.

(3) Temporary adjustment to work schedule/hours.

g. In cases where a PFA exists and the perpetrator and victim are employed by the same agency or are working in the same building, the agency will work to ensure a safe and productive work environment.

h. Incidents involving bomb threats and suspicious packages shall be handled in accordance with *Management Directive 720.7 Amended, Bomb Threats and Suspicious Packages*.

6. RESPONSIBILITIES.

a. Office of Administration, Office for Human Resources Management (OA/HRM), Bureau of Employee Benefits and Services (BEBS) shall:

(1) Provide overall policy guidelines to assist agencies in designing and/or implementing agency-specific workplace violence prevention and response programs, including the development of agency policies, training, and informational materials.

(2) Coordinate a commonwealth workplace violence reporting system and provide periodic reports to agencies on incidents and trends of workplace violence in commonwealth agencies.

(3) Coordinate the development of a workplace violence prevention training program which can be delivered through a variety of means.

(4) Function as a resource for the identification of workplace violence information and training resources.

(5) Provide assistance to agencies through SEAP debriefing services following a critical incident, in accordance with *Executive Order 1996-10*, *Management Directive 505.22*, and *Manual 505.3*, all titled *State Employee Assistance Program*.

(6) Ensure that SEAP has sufficient resources statewide to assist and support victims of domestic violence.

c. **Department of General Services (DGS)** shall:

(1) Develop and provide training or guidance on bomb threats and suspicious packages, in accordance with *Management Directive 720.7 Amended, Bomb Threats and Suspicious Packages*.

(2) Develop and provide training on selected workplace violence issues and other security measures, as appropriate.

(3) Respond to incidents of workplace violence in worksites under the jurisdiction of DGS where law enforcement assistance is requested.

d. **Agency Heads** shall:

(1) Designate an agency workplace violence coordinator and provide the name to BEBS. As appropriate, individual field/worksite workplace violence coordinators should also be designated and their names provided to BEBS.

(2) Ensure that the agency develops and implements an agency workplace violence prevention and response policy and program which are consistent with this management directive and *Manual 505.6, An Agency Guide to Workplace Violence Prevention and Response*.

(3) Provide necessary support and resources to the agency workplace violence prevention program.

(4) Create a workplace environment which encourages discussion of workplace violence issues and encourages employees who have filed a PFA to inform the agency human resources office so that appropriate safety precautions can be implemented.

(5) Ensure that all employees receive the required training on workplace violence prevention and response on an annual basis.

(6) Ensure that all reported incidents are investigated and that appropriate action(s) is taken when the investigation substantiates that workplace violence has occurred.

(7) Ensure that existing agency policies are applied in a flexible manner to support employees who self-disclose that they are victims of domestic violence, consistent with agency and commonwealth policy.

(8) Ensure that all incidents of workplace violence are reported to BEBS through the commonwealth's electronic workplace violence reporting system.

e. **Agency Workplace Violence Coordinators** shall:

(1) Implement the provisions of this management directive and the agency's workplace violence prevention policy and program.

(2) Identify, in conjunction with agency management, the types of workplace violence prevention initiatives which are appropriate to meet agency needs.

(3) Coordinate with BEBS, Capitol Police, State Police, local law enforcement authorities, and other resources to obtain appropriate advisory services and training to meet the agency's needs.

(4) Serve as a resource for managers, supervisors and employees regarding workplace violence prevention and response issues, including the development of worksite plans.

(5) Coordinate the delivery of workplace violence prevention training and the dissemination of information regarding workplace violence prevention.

(6) Ensure that all employees are aware of the internal agency procedures for reporting incidents of workplace violence.

(7) Ensure that all reported incidents of workplace violence are investigated, and as appropriate, participate as a member of the agency's assessment team in accordance with *Manual 505.6, An Agency Guide to Workplace Violence Prevention and Response*.

(8) Report all incidents of workplace violence through the commonwealth's electronic workplace violence reporting system.

(9) Notify the agency SEAP coordinator of all serious incidents of workplace violence so that appropriate SEAP services may be considered, and ensure that all agency policies and procedures regarding workplace violence include information regarding the availability of SEAP.

(10) Notify the agency human resources director and agency legal office of all instances where the agency has been notified that an employee has filed a PFA against another person, ensure that appropriate safety precautions are implemented, and work with the manager/supervisor to make appropriate job-related adjustments.

f. **Managers and Supervisors** shall:

(1) Ensure employees are provided with and are familiar with the commonwealth and agency workplace violence prevention policies, agency specific information and any local worksite plans.

(2) Be proactive in their supervisory responsibilities to minimize risk of workplace violence consistent with operational considerations, and initiate corrective action and discipline where warranted.

(3) Encourage any employee that may be experiencing personal problems to contact SEAP.

(4) Consult the agency human resources office when employees show signs of inappropriate workplace behavior, show warning signs of potential workplace violence, or demonstrate behavior that may be workplace violence.

(5) Report all incidents of workplace violence in accordance with agency procedures.

(6) Notify the agency workplace violence coordinator when an employee self-discloses that he or she has a PFA against another individual, treat the information in a confidential manner, and encourage the employee to seek assistance through SEAP.

g. **Agency SEAP Coordinators** shall:

(1) Notify BEBS following serious incidents of workplace violence and request a critical incident stress debriefing where warranted.

(2) Inform managers and supervisors of the resources available through SEAP should an incident of workplace violence occur.

h. **Employees** shall:

(1) Read and be familiar with the commonwealth and agency workplace violence prevention policies and procedures, and be proactive in the prevention of workplace violence incidents.

(2) Immediately report all incidents of workplace violence to their supervisor.

(3) Consider notifying their supervisor or human resources office if they have a PFA against another individual so that the agency can take appropriate safety precautions.

7. PROCEDURES.

a. A copy of this directive shall be posted in all commonwealth-owned and leased office buildings.

b. Agencies are to use the procedures found in *Manual 505.6, An Agency Guide to Workplace Violence Prevention and Response*, for the development of a comprehensive workplace violence prevention and response program, including worksite assessments, development of local worksite plans, the formation of field and central office assessment teams where warranted, and periodic reviews of the effectiveness of the agency program.

c. Employees, supervisors, and managers who witness or experience any workplace violence situation, as defined in this directive, must report the incident through established agency reporting procedures.

d. All employees must receive training on workplace violence awareness and prevention on an annual basis, in addition to being provided a copy of the agency policy on workplace violence prevention.

e. Immediate action must be taken in the event of a workplace violence incident and appropriate emergency and law enforcement personnel should be contacted if the incident warrants.

f. Agencies must immediately report any serious or life threatening incidents of workplace violence, such as bomb threats, attacks with a weapon, rape, suicide and murder to BEBS via telephone or email, after emergency and law enforcement personnel have been notified and the situation contained.

g. The agency SEAP coordinator should contact BEBS following all serious incidents of workplace violence to make arrangements for any needed SEAP services.

h. Agencies must report all incidents of workplace violence to BEBS via the electronic system. Agencies must enter all incidents that are reported to them, regardless of whether the investigation determines that the incident represents workplace violence. Agencies may enter the reports at the conclusion of the investigation, or may enter the reports at the time the incident is brought to their attention and then later update the report once the investigation has been concluded.

This directive replaces, in its entirety, *Management Directive 205.33,* dated June 22, 1999 and *Management Directive 505.31,* dated May 31, 2004.

DEFENDANT - SMF

EXHIBIT 6

MANAGEMENT DIRECTIVE

Commonwealth of Pennsylvania
Governor's Office

Subject: Commonwealth of Pennsylvania Information Technology Acceptable Use Policy	***Number:*** 205.34 Amended
Date: January 22, 2016	***By Direction of:*** Sharon P. Minnich, Secretary of Administration
Contact Agency: Office of Administration, Office for Information Technology, Telephone 717.787.5440 Email ra-ITCentral@pa.gov	

This directive establishes policy, responsibilities, and procedures for the acceptable use of Information Technology (IT) resources by Authorized Users. Marginal dots are excluded due to major changes.

1. **PURPOSE.** To establish policy, responsibilities, and procedures to provide Authorized Users with guidelines for, restrictions upon, and standards for the acceptable use of IT Resources. Covered IT Resources include those that are connected from any location to the commonwealth's computer systems including the Metropolitan Area Network (MAN), which is the commonwealth's computer network that spans the state and provides connectivity for Local Area Networks (LANs), as well as the internet; and IT Resources that are not connected to or used in conjunction with the MAN.

2. **SCOPE.** This directive applies to all Authorized Users of all departments, boards, commissions, and councils (hereinafter referred to as "agencies") under the Governor's jurisdiction and contractors, consultants, volunteers, and any other Authorized User who utilizes or has access to IT Resources.

3. **OBJECTIVE.** To ensure that all Authorized Users that have access to IT Resources are made aware of and comply with the standards and policy set forth in this directive and in Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology (IT) Resources.

4. **DEFINITIONS.**

   a. **Authorized Users.** Commonwealth of Pennsylvania employees, contractors, consultants, volunteers or any other user who utilizes or has access to IT Resources.

EXHIBIT IV

b. Electronic Communication System. Any method of electronic communication or information system that generates, stores, transmits, or displays information, including, but not limited to:

(1) The commonwealth's Metropolitan Area Network;

(2) Local Area Networks;

(3) The Internet;

(4) News groups;

(5) Bulletin board systems;

(6) Intranets;

(7) Social media;

(8) Blogs;

(9) Computer hardware;

(10) Software programs;

(11) Applications;

(12) Voice mail systems;

(13) Telephones;

(14) Faxes;

(15) Radio;

(16) Cellular and smartphones;

(17) Electronic mail and messaging systems;

(18) Instant Messaging;

(19) Text Messaging;

(20) Cloud storage solutions;

(21) Video conferencing and transmissions; and

(22) Electromagnetic, photo-electronic, and other electronic media or devices.

c. **IT Resource.** Any commonwealth computer system, Electronic Communication System, or electronic resource used for electronic storage and/or communications, including, but not limited to:

(1) Servers;

(2) Laptops;

(3) Desktop computers;

(4) Copiers;

(5) Printers;

(6) Wired or wireless telephones;

(7) Cellular phones or smartphones;

(8) Tablets;

(9) Wearables;

(10) Pagers;

(11) All other mobile devices; and

(12) Commonwealth contractor-provided IT Resources of all kinds.

5. POLICY.

a. **Authorized Users of IT Resources are required to understand and abide by this directive and the Acceptable Use Standards.** These Acceptable Use Standards are designed to prevent use that may be illegal, unlawful, abusive, or which may have an adverse impact on the commonwealth or its IT Resources. In addition, they identify for Authorized Users the permissible and effective uses of IT Resources. Authorized Users are encouraged to assist in the enforcement of these Acceptable Use Standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer. Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology (IT) Resources, sets forth additional information about the permissible scope of usage of IT Resources.

b. **Abuse or misuse of IT Resources will have consequences.** The improper use of commonwealth IT Resources by employees or volunteers may result in disciplinary action, up to and including termination of employment or volunteer status, depending on the circumstances of the incident. The improper use of IT Resources by contractors or consultants may result in disciplinary action that may include termination of engagement, and other formal action under the terms of the applicable contract or debarment under the Contractor Responsibility Program set forth in *Management Directive 215.9, Contractor Responsibility Program*. When warranted, the commonwealth or its agencies may pursue or refer matters to other appropriate authorities for investigation regarding potential violation of local, state, or federal laws through the misuse of IT Resources.

c. **Ownership of IT Resources.** All data and records, including those pertaining to computer use, Internet use, email communication, voicemail communication, text messages, and other electronic communication (whether sent, received, or stored), as well as the content of such communications, are presumed to be the sole and exclusive property of the commonwealth. Individual Authorized Users do not control the access to or the use of such data or records. In addition, Authorized Users have no property or other rights to any or all related physical equipment, hardware, and software applications that are provided, stored, or otherwise utilized in connection with IT Resources.

d. **Authorized Users should have no expectation of privacy when using IT Resources.** At its discretion, executive level or human resources staff or their authorized designees may access IT Resources in any way, including to retrieve, search, trace, audit, monitor and review any files, data, or records which are stored on or accessed through IT Resources, as well as, data or records related to IT Resource usage, including Internet records or email communications, for business purposes, or in order to determine compliance with the provisions of this directive or any other directive, personnel policy or applicable local, state, or federal law. Agency heads may determine who may access these files, data, and records, including, but not limited to, executive level staff, legal staff, human resource management staff, network or security system administrators, individuals in the Authorized User's chain of command or others, including law enforcement. Files, data, and records which are stored on IT Resources together with records of IT Resources use may be reviewed at any time and are routinely backed up and stored without the user's knowledge. As such, Authorized Users should have no expectation of privacy in any electronic files, data, or records stored on or accessed through IT Resources nor should an Authorized User have any expectation of privacy in any communications sent or received via, or stored within, IT Resources.

e. **IT Resources are subject to monitoring or other access by authorized commonwealth personnel.** All IT Resources and files, data, or records stored on or accessed through IT Resources may be accessed in any way (including but not limited to being traced, audited, monitored, reviewed, logged, blocked, searched, retrieved, or recorded) by authorized commonwealth personnel with or without notice to the Authorized User.

f. **Use of an IT Resource by an Authorized User is deemed to be consent to all access by authorized commonwealth personnel.** By using an IT Resource, Authorized Users consent to all access by authorized commonwealth personnel, including but not limited to use being traced, audited, monitored, reviewed, logged, blocked, searched, retrieved, or recorded, with or without notice.

g. **Authorized Users may not access unauthorized data and should take measures to protect the security of their data.** As part of the privilege of being an Authorized User, Authorized Users may not attempt to access any data or programs contained on commonwealth systems for which they do not have authorization or explicit consent. Authorized Users must use passwords and/or encryption in a manner that is consistent with commonwealth policy. Utilization of special passwords or encryption does not, however, guarantee the confidentiality of any electronic communication or of any file, data, or record stored or accessed through IT Resources. Authorized Users must keep passwords secure and must not share them with others.

h. **IT Resources are intended for business use and should be used primarily for that purpose.** IT Resources are tools that the commonwealth has made available for commonwealth business purposes. Where personal use of IT Resources does not interfere with the efficiency of operations and is not otherwise in conflict with the interests of the commonwealth, reasonable use for personal purposes will be permitted in accordance with standards established for business use. Such personal use shall be limited, occasional, and incidental. Any personal use which is inconsistent with commonwealth policy regarding availability or capability of IT Resources, or inappropriate content of communications as defined by this policy is prohibited.

i. **IT Resources must never be used in a manner that violates other commonwealth directives and policies.** All use of IT Resources must conform with *Executive Order 1980-18, Code of Conduct*, *Management Directive 505.7, Personnel Rules*, and commonwealth policies on nondiscrimination and prohibition of sexual harassment. Violations of these issuances and policies through IT Resources will be treated in the same manner as other violations.

j. **All Authorized Users must be provided with this directive.** All current commonwealth employees must be provided a copy of this policy. All new employees must review this policy during new employee orientation. All non-commonwealth employee Authorized Users must review this policy prior to their use of and access to commonwealth IT Resources. Copies may be provided either electronically or in hard copy.

k. **All Authorized Users must sign an Acknowledgement of Receipt Form.** On an annual basis agencies must obtain signed user agreements from Authorized Users **prior** to granting access to IT Resources. Employees or volunteers shall sign Enclosure 2 to this directive, Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Employee or Volunteer Form. Contractors and consultants shall sign Enclosure 3 to this directive, Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Contractor or Consultant Form.

l. **Each agency must maintain copies of the agreement signed by each Authorized User in that agency.** Completed user agreements shall be maintained as part of the employee's Official Personnel Folder. Alternately, Authorized Users may sign and agencies may store these agreements in an electronic format consistent with *Management Directive 210.12, Electronic Commerce Initiatives and Security*, and *ITP-SEC006, Commonwealth of Pennsylvania Electronic Signature Policy*. Signed agreements must be accessible to individuals who are authorized to view or use the documents.

m. **Requests for electronic records should be treated in the same manner as paper records.** Requests for records pertaining to IT Resources must be addressed consistent with all laws, directives, or policies that would apply to the same information if maintained in a non-electronic format. These requests should be referred to agency legal counsel and/or the Agency Open Records Officer, as appropriate.

n. **This amended directive supersedes prior or inconsistent policies.** This policy supersedes any existing IT, Internet and/or email use policy issued by agencies under the Governor's jurisdiction that is inconsistent with this directive, unless specific exemptions are granted by the Secretary of Administration or designee. Approved labor agreements, side letters or current practices should be applied in a manner to effectuate both this policy and any such agreement, side letter or current practice. In cases where a provision of an approved labor agreement, side letter or current practice cannot be reconciled with this policy, the former shall control. Agencies may develop supplemental IT, Internet and/or email use policies only with the approval of the Secretary of Administration or designee.

6. **RESPONSIBILITIES.**

a. **Agency** shall:

(1) Provide either a hard copy or electronic copy of this directive to Authorized Users.

(2) Ensure that Authorized Users have signed the user agreement.

(3) Maintain a copy of the signed user agreement for Authorized Users.

b. **Authorized Users** shall:

(1) Understand the permissible scope of usage of IT Resources.

(2) Sign the user agreement.

c. **Enterprise Information Security Office** may:

(1) Conduct system audits and compliance reviews of adherence to this directive.

(2) Prevent and respond to cyber security incidents.

(3) Assist human resources staff in conducting investigations involving the alleged misuse of IT Resources.

(4) Assist in data retrieval and analysis for any records requests.

7. **RELATED GUIDANCE/REFERENCES.** Additional technical standards for IT Resources usage will be published in the Office of Administration, Office for Information Technology (OA/OIT), Information Technology Policies are available on the OA/OIT website.

Enclosure 1 - Commonwealth Acceptable Use Standards for Information Technology (IT) Resources
Enclosure 2 – Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Employee or Volunteer Form
Enclosure 3 – Commonwealth IT Resources Acceptable Use Policy User Agreement Commonwealth Contractor or Consultant Form

This directive replaces in entirety, *Management Directive 205.34*, dated November 17, 2011.

COMMONWEALTH ACCEPTABLE USE STANDARDS FOR INFORMATION TECHNOLOGY (IT) RESOURCES

Each Authorized User must comply with *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy* and the following Acceptable Use Standards when using IT Resources:

AUDITING, MONITORING AND REPORTING

All IT Resources and files, data, or records stored on or accessed through IT Resources may be accessed in any way (including but not limited to being traced, audited, monitored, reviewed, logged, blocked, searched, retrieved, or recorded) by authorized commonwealth personnel with or without notice to the Authorized User.

Authorized Users, therefore, should have no expectation of privacy in any files, data or records stored on or accessed through IT Resources, nor should they have any expectation of privacy in any electronic communication sent or received via, or stored within, IT Resources. By using IT Resources, the user authorizes any access to IT Resources by the commonwealth.

Authorized Users are encouraged to assist in the enforcement of these Acceptable Use Standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer.

DISCIPLINE OR OTHER CONSEQUENCES OF MISUSE

The improper use of IT Resources by employees or volunteers may result in disciplinary action, up to and including termination of employment or volunteer status, depending on the circumstances of the incident. The improper use of IT Resources by contractors or consultants may result in disciplinary action that may include termination of engagement, other formal action under the terms of the applicable contract, or suspension or debarment under the Contractor Responsibility Program. When warranted, the commonwealth or its agencies may pursue or refer matters to other appropriate authorities for investigation regarding potential violation of local, state, or federal laws through the misuse of IT Resources.

GENERAL IT RESOURCES USE

a. As part of the privilege of being an Authorized User, Authorized Users may not attempt to access any data or programs contained on commonwealth systems for which they do not have authorization or explicit consent.

b. Authorized Users are strictly responsible for maintaining the confidentiality of their commonwealth or agency account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes (such as multi-factor authentication methods).

c. Authorized Users may not make unauthorized copies of software.

d. Authorized Users may not use non-standard shareware or freeware software without agency IT management approval.

e. Authorized Users may not purposely engage in activity that may: harass, threaten, or abuse others; degrade the performance of IT Resources; deprive an Authorized User of access to an IT Resource; obtain extra IT Resources beyond those allocated; or circumvent IT Resource security measures.

f. Authorized Users may not use IT Resources to engage in personal, for-profit transactions or business, or to conduct any fundraising activity not specifically sponsored, endorsed, or approved by the commonwealth.

g. Authorized Users may not engage in illegal activity in connection with their use of IT Resources, including, but not limited to downloading, installing, and/or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Authorized Users may not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on IT Resources, unless they are authorized to do so.

h. Authorized Users may not access, create, store, transmit, post, or view material that is generally considered to be inappropriate or personally offensive or which may be construed as discriminatory or harassing, including sexually suggestive, pornographic, or obscene material.

i. Authorized Users are personally responsible for the security of authorized portable and mobile IT Resources and devices. Care must be exercised to ensure these devices are secured and not lost, stolen or otherwise accessed in an unauthorized manner.

j. Authorized Users may not store non-public information on IT Resources, if those IT Resources may be removed from commonwealth facilities without prior approval from the agency Secretary or designee.

k. Authorized Users shall use commonwealth approved electronic communication systems primarily for commonwealth business.

l. Authorized Users shall use only commonwealth approved encryption methods to encrypt information, as appropriate.

m. Authorized Users shall use only commonwealth approved storage devices or storage solutions.

n. Authorized Users may only store or transmit commonwealth content, files, data or any other type of information on or through an IT Resource that is commonwealth-provided or commonwealth-approved..

INTERNET USE

All security policies of the commonwealth and its agencies, as well as policies of Internet websites being accessed, must be strictly adhered to by Authorized Users.

Software

In connection with Authorized Users' use of and access to IT Resources:

a. All software used to access IT Resources must be part of the agency's standard software suite or approved by the agency IT department. This software must incorporate all vendor provided security patches.

b. All files downloaded from the Internet must be scanned for viruses using the approved commonwealth distributed software suite and current virus detection software.

c. All software used to access the Internet shall be configured to use an instance of the commonwealth's standard Internet Access Control and Content Filtering solution.

Access Control and Authorization

Agencies should authorize access to the Internet using commonwealth IT Resources through the utilization of a user ID/password system. Security violations can occur through unauthorized access, and all possible precautions should be taken to protect passwords. Authorized Users are responsible for activity and communications, including but not limited to email, voicemail, text messages, data, and any other electronic communications transmitted under their account.

Incidental Use

a. IT Resources are communication tools that the commonwealth has made available for commonwealth business purposes. Where personal use of these resources does not interfere with the efficiency of operations and is not otherwise in conflict with the interests of the commonwealth, reasonable use for personal purposes will be permitted in accordance with standards established for business use. Such personal use shall be limited, occasional, and incidental.

b. Incidental personal use of Internet access is restricted to Authorized Users; it does not extend to family members, other acquaintances, or any other persons.

c. Access to IT Resources that are home-based, e.g., accessing the Internet from an agency owned, home-based computer, must adhere to all the same policies that apply to use from within agency facilities.

d. Employees may not allow family members or other non-employees to access commonwealth provided home-based IT Resources.

e. Incidental use must not result in direct costs to the commonwealth.

f. Incidental use must not interfere with the normal performance of an Authorized User's work duties.

g. Incidental use may not risk legal liability for, or embarrassment to, the commonwealth.

h. All files and documents located on IT Resources, including personal files and documents may be accessed and retrieved in accordance with this policy. In addition, it should be understood that such documents may be subject to disclosure under the *Right-to-Know Law, 65 P.S. §§ 67.101—67.3104*, and other laws.

Acceptable Use of the Internet

Accepted and encouraged use of the Internet for Authorized Users on IT Resources includes, but is not limited to, the following:

a. Access, research, exchange, or posting of information that relates to the assigned job duties of an Authorized User for carrying out commonwealth business.

b. Promotion of public awareness in regard to commonwealth law, agency services, and public policies.

c. Posting of agency information that has been authorized by appropriate management.

Acceptable use of Instant Messaging (IM)

a. Only Authorized Users who have been granted agency level approval to utilize IM technology may use IM software, and they may use it only to communicate internally across the commonwealth MAN in a manner directly related to an Authorized User's job responsibilities.

b. IM software that is utilized by commonwealth Authorized Users must be part of the determined enterprise standard software solution.

c. IM software is only to be used to conduct state business that produces records that have little or no documentary or evidentiary value and that need not be set aside for future use. These records are subject to the provisions of *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program* and *Manual 210.9, The Commonwealth's General Records Retention and Disposition Schedule*, Items G001.021, Transitory Records and G001.025, Transitory Files Confidential.

Acceptable use of Social Media

a. Social Media may include, but are not limited to, blogs, RSS, discussion boards, social networking, wikis, video sharing sites, mashups, and social tagging.

b. Only Authorized Users who have been granted agency level approval to do so may utilize Social Media, and only if the use is directly related to an Authorized User's job responsibilities. Please refer to *Management Directive 205.42, Social Media*.

c. Social Media may be used only to conduct commonwealth business that produces records that have little or no documentary or evidentiary value and that need not be set aside for future use. These records are subject to the provisions of *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program* and *Manual 210.9, The Commonwealth's General Records Retention and Disposition Schedule*, Items G001.021, Transitory Records and G001.025, Transitory Files Confidential.

Acceptable Use of Mobile Technologies

Authorized Users shall ensure that information on mobile devices is not compromised by:

a. Securing mobile devices from access by unauthorized persons, through the use of locking devices, passwords, or other appropriate protection;

b. Ensuring that unauthorized persons do not view information on the display screen;

c. Refraining from checking devices into airline luggage systems, with hotel porters, or from using other unsupervised handling or storage processes;

d. Securing or maintaining possession of mobile devices at all times; and

e. Immediately reporting a lost or stolen mobile device to their supervisor.

Acceptable Use of Cloud Storage Solutions

a. Cloud storage solutions enable convenient, on-demand network access to a shared pool of configurable computing resources such as storage that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud storage solutions are intended for business use and shall be used primarily for that purpose.

b. Cloud storage solutions must never be used in a manner that violates other commonwealth directives and policies. The use of cloud storage solutions must conform with *Executive Order 1980-18, Code of Conduct*, *Management Directive 505.7, Personnel Rules*, and the *Management Directive 205.34 Amended, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*. Violations of these issuances and policies through IT Resources will be treated in the same manner as other violations.

c. All files and documents located in cloud storage solutions are generally owned by the commonwealth and may be accessed and retrieved in accordance with this policy. In addition, it should be understood that such documents may be subject to requests for disclosure under the *Right to Know Law, 65 P.S. §§ 67.101—67.3103*, and other similar laws.

d. Users will only access those cloud storage solutions which have been authorized for their use.

e. Users who obtain a password and ID for a cloud storage solution shall keep that password confidential. Commonwealth policy prohibits the sharing of user IDs or passwords obtained for access to network and cloud storage resources.

f. Users are responsible for the use of their individual cloud storage accounts and should take all reasonable precautions to prevent others from being able to use their account, including coworkers, friends, or family.

g. Any user placing sensitive data into Cloud Storage Solutions must (in concert with his or her chain of command and/or Chief Counsel's Office, as appropriate) evaluate the risk to the data's security, privacy, and availability. No commonwealth policy or procedure may be violated via use of a Cloud Storage Solution unless that policy or procedure is itself explicitly waived.

EMAIL USE

Usage

a. When sensitive material is sent electronically via email, it is important to verify that all recipients are authorized to receive such information and to understand that email is not fully secure and/or private, except where appropriate security applications are used, e.g. data encryption.

b. Users should understand that messages can be quickly and easily copied and may be forwarded inappropriately.

c. Where it is necessary to transmit commonwealth proprietary or restricted information beyond the commonwealth email network, the messages should be protected by encryption. Authorized Users should contact their agency Network Coordinator or IT Coordinator for assistance if encryption is needed.

d. Email messages to be transmitted outside of the United States should comply with local laws governing international transmission of data as well as United States export control regulations. For assistance, Authorized Users should contact their Network Coordinator or IT Coordinator, who may receive technical assistance from the Office of Administration, Office for Information Technology (OA/OIT).

e. The agency head or designee should determine specific agency policy regarding business information which is determined to be too confidential or sensitive to be transmitted via email.

f. All user activity and electronic communication, including the contents of such communication, including but not limited to, email, voicemail, text messages and data, on IT Resources is subject to access, including tracking, blocking, logging, auditing, monitoring, retrieving, and reviewing as described more fully in this directive.

g. Authorized Users shall use email addresses assigned to them primarily for work-related purposes. Authorized Users may not use their commonwealth e-mail address to register or subscribe for any product or service that is not work-related.

h. Authorized Users shall not forward work related emails, calendar items or documents to their personal non-commonwealth email addresses. In the event that a provision of an approved labor agreement, side letter or current practice cannot be reconciled with this policy, the former will control.

Access Control and Authorization

a. Only Authorized Users may use IT Resources to send or view email or access the commonwealth's email systems.

b. Only after agreement to abide by all applicable rules of the system, including this directive and its related Acceptable Use Standards, shall access to commonwealth email be granted to commonwealth employees, contractors, consultants, and volunteers, in their capacity as Authorized Users.

c. An Authorized User may not access the email or account of another Authorized User. This restriction does not apply to system administrators and management staff in the Authorized User's chain of command authorized to access email for legitimate business purposes, to effectuate *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*.

d. In accordance with agency policy, Authorized Users shall use password protection to limit access to email files. Authorized Users shall safeguard their passwords so that unauthorized users do not have access to their email. Authorized Users are responsible for all messages transmitted and originating under their account.

Message Retention

All messages, including email, text messages, and voicemail messages are subject to the appropriate records retention and disposition schedules and the provisions of *Management Directive 210.5, The Commonwealth of Pennsylvania State Records Management Program*.

Email Security Issues, Worms, and Viruses

Email and attachments to email are sources of computer security issues. All Authorized Users should act in accordance with the latest IT Policies regarding containment methods for computer viruses and any security alert emails from agency HR or IT.

Maintaining Professionalism

Every Authorized User who uses IT Resources is responsible for ensuring posted messages and other electronic communications are professional and businesslike. As a way to impose personal restraint and professionalism, all Authorized Users should assume that whatever they write may at some time be made public. Authorized Users should follow the following guidelines:

- Be courteous and remember that you are representing the commonwealth with each email message sent.
- Review each email message before it is sent and make certain that addresses are correct and appropriate. Use spell check before sending.
- Consider that each email message sent, received, deleted, or stored has the potential to be retrieved, seen, and reviewed by audiences, including the general public, who were not the intended recipients of the message.
- Ensure that content is appropriate and consistent with business communication; avoid sarcasm, exaggeration, and speculation which could be misconstrued. Remember that intonation and inflection are lost in email.
- Be as clear and concise as possible; be sure to clearly fill in the subject field so that recipients of email can easily identify different email messages.

Electronic Message Distribution, Size, and Technical Standards

a. Authorized Users should receive authorization from their supervisors before wide scale "broadcasting" an email bulletin to groups of employees.

b. The use of "reply to all" should be avoided unless it is appropriate to respond to all addressees.

c. Authorized Users wishing to send email bulletins to all commonwealth or agency employees must first obtain authorization from agency management.

d. Email messages should be brief, and attachments to email messages should not be overly large. Agency IT staff will inform Authorized Users of limitations on the size of email messages and attachments. OA/OIT periodically will provide technical standards and guidance to agencies through IT Policies on the technical capacities of the commonwealth email system and limitations on email message size. Technical standards will be provided in areas such as file size and backup procedures, and will be available on the OA/OIT website at http://www.oit.state.pa.us.

UNACCEPTABLE USES OF IT RESOURCES

The following are examples of impermissible uses of IT Resources. This list is by way of example and is not intended to be exhaustive or exclusive. Authorized Users are prohibited from:

- Accessing, creating, storing, transmitting, posting, or viewing material that is generally considered to be inappropriate or personally offensive or which may be construed as harassing, including sexually suggestive, pornographic, or obscene material.
- Accessing, creating, storing, transmitting, posting, or viewing material that expresses or promotes discriminatory attitudes toward race, gender, age, nationality, religion, or other groups including, but not limited to, protected groups identified in *Executive Order 2003-10, Equal Employment Opportunity*.
- Engaging in personal, for-profit transactions or business, or conducting any fundraising activity not specifically sponsored, endorsed, or approved by the commonwealth.
- Participating in Internet activities that inhibit an employee's job performance or present a negative image to the public, such as auctions, games, or any other activity that is prohibited by directive, policy, or law.
- Attempting to test or bypass the security ("hacking" or "cracking") of IT Resources or to alter internal or external IT Resource security systems.
- Participating in or promoting computer sabotage through the intentional introduction of computer viruses, worms, or other forms of malware, i.e. malicious software.
- Promoting, soliciting, or participating in any activities that are prohibited by local, state, or federal law or the commonwealth rules of conduct.
- Violating or infringing the rights of any other person.
- Using any other Authorized User's password and/or equipment to conduct unacceptable activities on IT Resources.

- Harassing or threatening activities including, but not limited to, the distribution or solicitation of defamatory, fraudulent, intimidating, abusive, or offensive material.
- Transmitting or soliciting any proprietary material, such as copyrighted software, publications, audio, or video files, as well as trademarks or service marks without the owner's permission.
- Promoting or participating in any unethical behavior or activities that would bring discredit on the commonwealth or its agencies.
- Downloading and/or installing any unapproved software.
- Transmitting or posting any messages that intentionally misrepresent the identity of the sender, hide the identity of the sender, or alter a sender's message.
- Sending or forwarding commonwealth information or records through non-commonwealth email or webmail accounts. Examples of non-commonwealth email accounts include, but are not limited to, Hotmail, Yahoo mail, Gmail, or email provided by other Internet service providers.
- Sending, forwarding, or storing commonwealth information or records utilizing non-commonwealth accredited mobile devices. Examples of mobile devices include, but are not limited to:
    - tablets, smart phones, pagers, wearables, and cellular telephones.
- Participating in any other Internet or email use that is deemed inappropriate by the commonwealth and/or its agencies and is communicated as such to Authorized Users.
- Using or disclosing confidential material covered by law or commonwealth policy.

COMMONWEALTH IT RESOURCE ACCEPTABLE USE POLICY USER AGREEMENT - COMMONWEALTH EMPLOYEE OR VOLUNTEER

This user agreement does not prohibit employees from performing authorized job duties.

I have read the attached *Management Directive 205.34, Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*, and Enclosure 1, Commonwealth Acceptable Use Standards for Information Technology, and in consideration of the Commonwealth of Pennsylvania making its IT resources available to me, I agree to abide by the requirements set forth therein. I understand that disciplinary action, up to and including termination, may be taken if I fail to abide by any of the requirements of this directive.

I further understand that my commonwealth IT resource usage, including electronic communications such as email, voice mail, text messages and other data and records, may be accessed and monitored at any time, with or without advance notice to me. By signing this agreement, I specifically acknowledge and consent to such access and monitoring.

I further understand that if I have any questions regarding this directive, I am required to ask for clarification from my supervisor or my agency human resource representative.

Printed Name: NANCY LEWEN

Employee Number: 00714579

Signature: [signature]

Date: 12-20-2014

Agency: DMVA/PSSH

Bureau/Facility: PSSH

Division/Section: Nursing

Mailing/Email Address: nlewen@pa.gov

Work Phone: 814-871-4531

Optional Agency Approval:

Date:

EXHIBIT N

DEFENDANT - SMF

EXHIBIT 7

DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
OFFICE OF THE ADJUTANT GENERAL
COMMONWEALTH OF PENNSYLVANIA
FORT INDIANTOWN GAP
ANNVILLE, PENNSYLVANIA 17003-5002
www.dmva.state.pa.us

TAGPA

19 July 2011

Standards of Conduct and Work Rules

The effective operation of the Department of Military and Veterans Affairs requires that employees maintain the highest personal Standards of Conduct and comply with established Work Rules. The rules are necessary to protect the health and safety of employees, to maintain work efficiency, and to promote public confidence and trust in the Department of Military and Veterans Affairs and Commonwealth government.

These work rules constitute the general rules applicable to employees of the Department of Military and Veterans Affairs. Additional work rules may be promulgated which concern individual positions, classifications and/or work units when such rules are required by the nature of the work performed. Likewise, the work rules do not constitute the entire list of violations for which employees must comply. Other rules are provided by Federal statute, by Pennsylvania Code, and by administrative procedures established by management for operational reasons. Violations of these rules will also result in appropriate disciplinary action.

Questions concerning the applicability or interpretation of the Work Rules should be referred to appropriate supervisors.

The following acts or conduct are specifically prohibited:

Work Performance

1. Neglect of duty or responsibility, including, but not limited to:
   a. Failure to perform assigned tasks or a legitimate work assignment.
   b. Failure to maintain a current license or certification as required by the job title or applicable regulations.
   c. Failure to complete mandatory training as directed.
   d. Failure to provide treatment and medication to a resident as directed.
   e. Dishonesty, including the falsification of reports and records such as medication or medical records, personnel, payroll, time and attendance, leave, employment applications, etc.
   f. Failure to treat residents of the veterans homes with dignity and respect, or any action which puts a resident in possible harm and/or violates the Department's Prevention of Resident Abuse Policy.

EXHIBIT H

g. Failure to document residents' medications after administration.

h. Failure to properly issue medication, or transcription error.

i. Failure to perform supervisory duties.

j. Sleeping or inattentiveness during working hours.

k. Unauthorized use of time during working hours.

l. Leaving assigned workstation without permission.

m. Refusal to work assigned overtime.

2. Unsatisfactory performance.

3. Insubordination, disobedience, failure or refusal to follow the written or oral instructions of supervisory authority, or to carry out legitimate work assignments or disrespectful conduct toward supervisors.

4. Disclosure of confidential information and records to unauthorized parties.

Time and Attendance

1. Failure to follow the time and attendance rules, including, but not limited to:
   a. Charges of an unauthorized absence (AW).

   b. Failure to report for or complete an overtime shift.

   c. Leaving the workplace before the scheduled end time of a shift.

   d. Failure to follow call-off policies and procedures.

   e. Failure to report promptly at the starting time of a shift, resulting in unexcused absence (Tardy).

   f. Failure to provide documentation for absence as required by a supervisor or by leave restriction notice.

   g. Unexcused or excessive absenteeism.

   h. Failure to observe the time limits of breaks and lunch periods, loafing, loitering, or engaging in unauthorized personal business on duty.

2. Misuse or abuse of sick leave.

DMVA Standards of Conduct and Work Rules

Safety Standards

1. Committing acts that endanger the safety or lives of others.
2. Failure to observe all safety rules and practices established by the Department and/or worksite, including the use of protective equipment and clothing.
3. Failure to observe all safety rules and practices in the operation of vehicles and equipment.
4. Unauthorized possession of firearms or other dangerous weapons on Department premises.
5. Reporting to work or working under the influence of narcotics or intoxicating beverages.
6. The unlawful manufacture, dispensing, possession, or use of alcohol and other controlled substances while performing official Commonwealth duty or on any Department property.
7. Smoking in unauthorized areas.
8. Physical violence, fighting, or creating a disturbance on Department premises.
9. Failure to adhere to the General Safety Standards as posted at all worksites.

Use of Property

1. Unauthorized operation or use of any machines, tools, equipment, vehicles, materials, or other Department or Federal property.
2. Loss of or damage to Commonwealth property through carelessness, neglect or indifferences.
3. Stealing/Theft
4. Unauthorized possession or use of government or private property, equipment, or materials.
5. Misuse or removal of Department property, records, or other materials from Department premises without proper authorization.
6. Unauthorized posting or removing of notices, signs, posters, or similar materials.
7. Unauthorized entry to Department or Commonwealth property or leased sites, or presence in an unauthorized area during working hours.

DMVA Standards of Conduct and Work Rules

Unauthorized Behavior

1. Any action which violates the Department or Commonwealth Workplace Violence Polices during working hours, or while on any Department property, including but not limited to inflicting bodily harm, threatening, intimidating, coercing, or interfering with fellow employees, supervisors, residents or the general public.

2. Threatening, intimidating, interfering with, or using abusive or profane language including ethnic slurs, towards fellow employees, subordinates, supervisors, residents or the general public, during working hours, or while on any Department property.

3. Inappropriate conduct or behavior towards fellow employees, supervisors, residents or the general public, during working hours, or while on any Department property.

4. The acceptance of loans, gifts, money, services, or other arrangements for personal benefit under any circumstances.

5. Any action which would reflect unfavorably on or discredit the Commonwealth or Department of Military and Veterans Affairs.

6. Failure to deal with fellow employees, residents and/or the public without regard to race, color, gender, gender identity and expression, age, disability, religious creed, ancestry, union membership, national origin or sexual orientation.

7. Favoritism or even the appearance of favoritism towards any resident of the veterans' home or subordinates.

8. Reporting to work unfit for duty.

9. Failure to inform supervisor of an arrest in accordance with the Governor's Code of Conduct.

10. Reporting false allegations or statements.

11. Interfering with or failure to cooperate with an official Department or Commonwealth investigation.

12. Any acts of retaliation against fellow employees, subordinates, supervisors, residents or the general public.

Wesley E. Craig
Major General, PAARNG
The Adjutant General

pennsylvania
DEPARTMENT OF MILITARY
AND VETERANS AFFAIRS

Standards of Conduct and Work Rules

Distribution and Acknowledgment

The Standards of Conduct and Work Rules are distributed to all Department of Military and Veterans Affairs' employees. Please sign your name on the line below to indicate that you have received a copy of the Standards of Conduct and Work Rules. This acknowledgement for will become part of your Official Personnel File.

You are cautioned to read and become familiar with the contents of the Standards of Conduct and Work Rules since violations may result in disciplinary action. If you have any questions regarding the contents, please contact your supervisor or your Human Resource Office.

NANCY LEWEN
Employee Name (Print)

12-20-2014
Date

Nancy Lewen
Employee Signature

File – Employee Official Personnel File

EXHIBIT
H